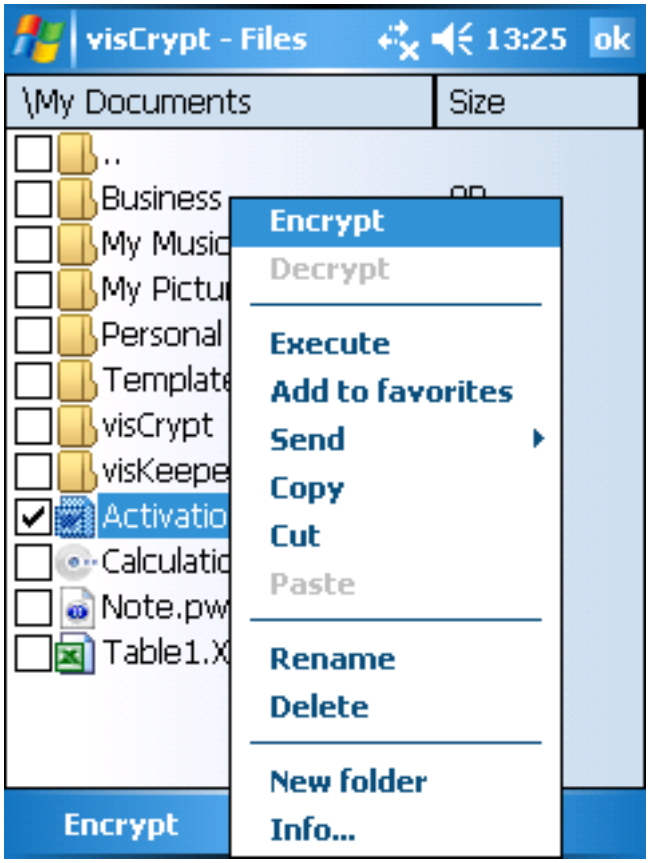
User manual visCrypt



SFR IT-ENGINEERING

www.visCrypt.com

June 2009

Contents

Foreword....3
Installation....4
Preliminary Remarks....4
Installation on the desktop PC....5
Starting the software after Installation....8
Program documentation....9
Starting visCrypt....9
The password wizard of visCrypt....10
The configuration file of visCrypt....13
The main screen....14
The list view....14
The context menu of the list view....15
The file menu....17
General....17
Information for files and folders....19
Settings....20
Information and activation....22
Log....23
Close visCrypt....24
Integration into Windows Mobile's file explorer....25
Uninstall visCrypt....26
The patented visual Key technology....28
visual Key: An alternative to text passwords....28
The process....28
Technical implementation....29
1. Regular allocation....29
2. Irregular allocation....30
License Agreement....31

Foreword

Dear Windows Mobile user,

When buying **visCrypt** you chose an innovative software solution for Windows Mobile Devices.

The combination with the patented and well-proven visual Key Technology grants that visCrypt is not only a comfortable but also a well protected encryption software.

This manual will lead you through the installation of visCrypt and acquaint you with the handling of the program. You will find information on the following topics:

1. Installation: The first chapter describes the installation of visCrypt.
2. Program documentation: Here you will find a detailed description of all features and settings of visCrypt.
3. The patented visual Key technology: This chapter is for those readers who want to learn more about how the program works and why the process is so secure.

Note: All functions of this software have been carefully tested on different devices. To our knowledge visCrypt runs faultlessly on all Windows Mobile Devices with Windows Mobile 2003 and higher.

SFR GmbH may not be held liable for any loss of data. Please read the information in the license agreement that will be shown during the installation (it may also be found in this manual).

visCrypt was developed for the operating systems Windows Mobile 2003/5/6. Incompatibilities with other applications are improbable, but they cannot be ruled out entirely.

Should you have any problems with our software, please visit www.visCrypt.com and read our FAQ.

Additionally you will find our forum there which helps to solve many problems.

Alternatively you may send us an e-mail to support@sfr-software.com.

We hope you will enjoy visCrypt!

Winfried Schöttler

- CEO SFR GmbH-

Installation

Preliminary Remarks

In order that you may install and use visCrypt as easily as possible, our software developers created a convenient installation routine and intuitive software handling. The installation routine will run almost completely software assisted. Only where you have to choose between certain options you will get a message which may be answered with one click.

The suggested settings have been thoroughly tested, and we recommend that you confirm them.

The software installation of visCrypt is effected in two steps, which are described in this document in detail.

visCrypt cannot be installed on Windows Mobile Devices directly. You must install it from your desktop PC by running the installation file.

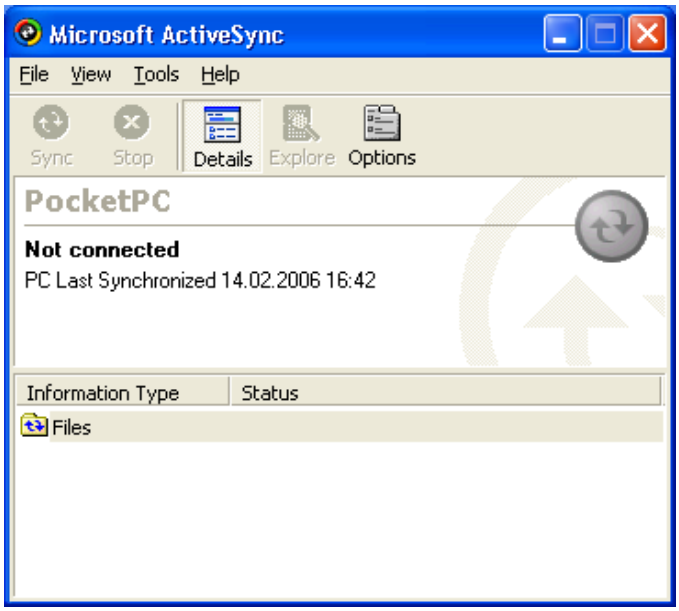
In order to install visCrypt a connection between desktop PC and Windows Mobile Device must be established.

Should you have any problems with this connection, please refer to your Windows Mobile Device's manual, or ask the manufacturer of your hardware.

The following steps apply to a connection established with the Microsoft software ActiveSync® or the Windows Mobile Devicecenter.

Installation on the desktop PC

Establish connection (Windows XP and older)

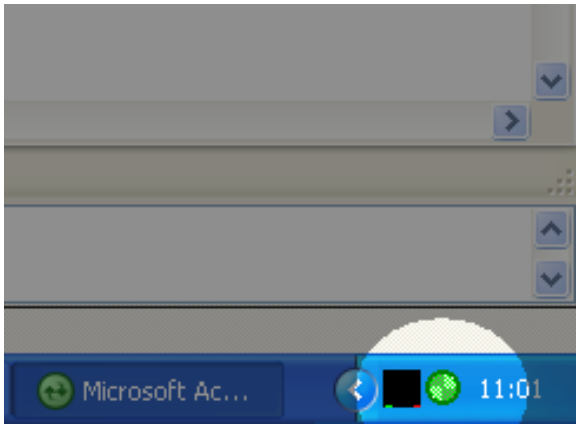


Establish an "ActiveSync"-connection between your PC and your Windows Mobile Device.

Pay attention to the **green control light**. It symbolizes an existing connection throughout the first installation step.

A **gray control light** means that there is no connection. In this case please try to reconnect.

Note: If you cannot establish an "ActiveSync"-connection, try restarting your PC with the Windows Mobile Device still connected.



Establish connection (Windows Vista)

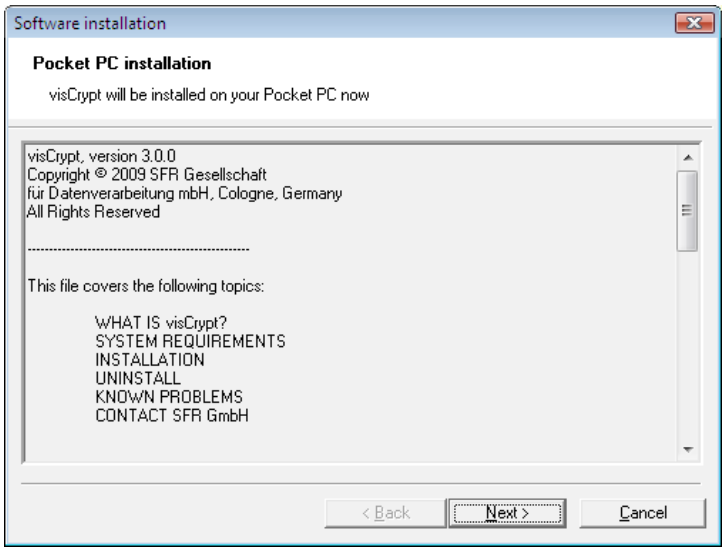
Establish a connection between your PC and your Windows Mobile Device.

In Windows Vista you must start the Windows Mobile Devicecenter.

If this software is not installed on your computer, you can download it from the Microsoft sites.

Please ensure the device keeps connected throughout the installation process by showing the status “Connected”.

Start Setup File



Start the installation file on your PC.

The installation routine will greet you with the "Welcome"-screen.

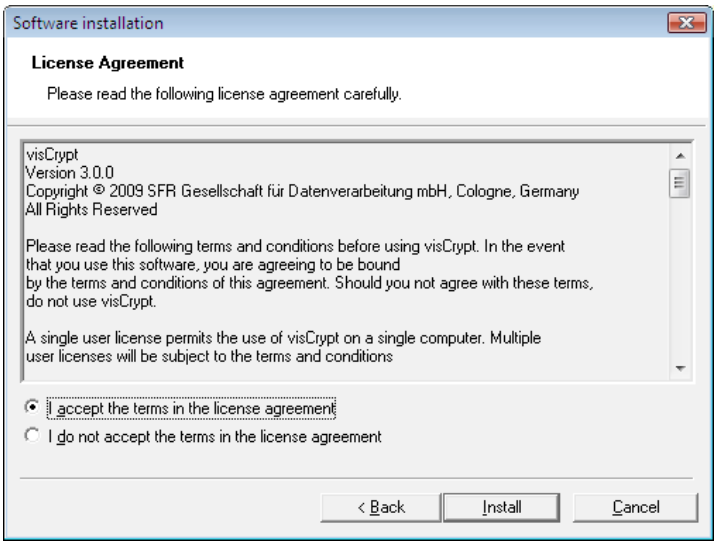
Please read it and confirm with "**Next**".

Accept license agreement

Finally you will be shown the license agreement for visCrypt.

If you want to install and use the software, please accept the license terms.

The regulations may also be found in this document.


Software installation
License Agreement
Please read the following license agreement carefully.
visCrypt
Version 3.0.0
Copyright © 2009 SFR Gesellschaft für Datenverarbeitung mbH, Cologne, Germany
All Rights Reserved
Please read the following terms and conditions before using visCrypt. In the event that you use this software, you are agreeing to be bound by the terms and conditions of this agreement. Should you not agree with these terms, do not use visCrypt.
A single user license permits the use of visCrypt on a single computer. Multiple user licenses will be subject to the terms and conditions
I accept the terms in the license agreement
I do not accept the terms in the license agreement
< Back
Install
Cancel

Software installation

visCrypt will now contact your Windows Mobile Device's operating system and begin with the actual software installation.

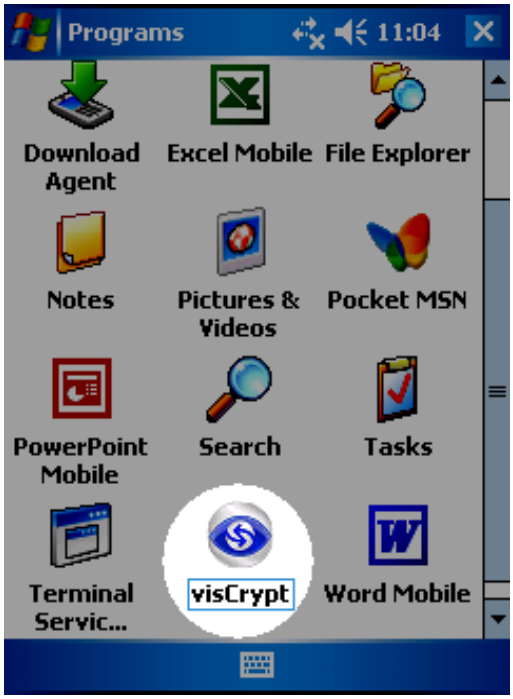
Define installation directory

Now you will be asked to define the directory for the installation of visCrypt on your Windows Mobile Device.

Finish copying process

When the copying is finished you will get a message. Please confirm this message with “OK”

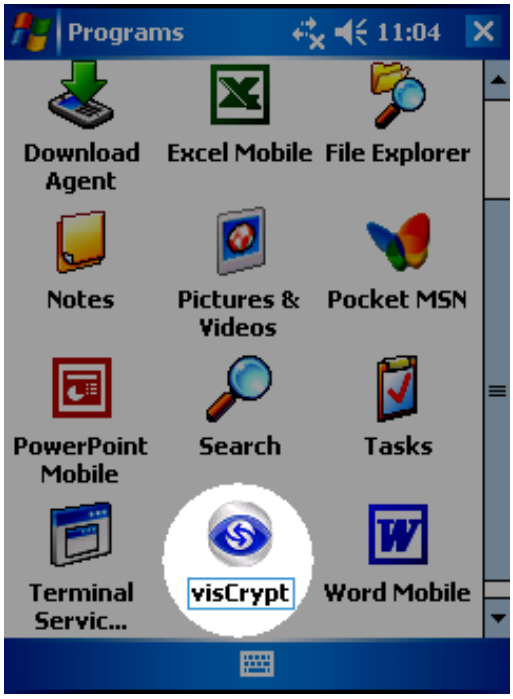
Starting the software after Installation



You may find visCrypt in the directory "**Program Files**" of your Windows Mobile Device.

Program documentation

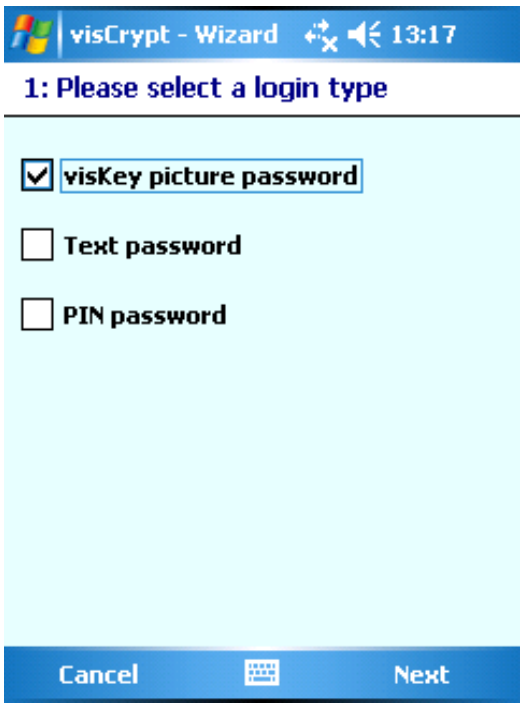
Starting visCrypt



If visCrypt is installed correctly on your Windows Mobile Device, you will find the icon to start the software in the folder „Program files" of your Windows Mobile Device.

After starting, visCrypt will ask you to enter your master password.

The password wizard of visCrypt



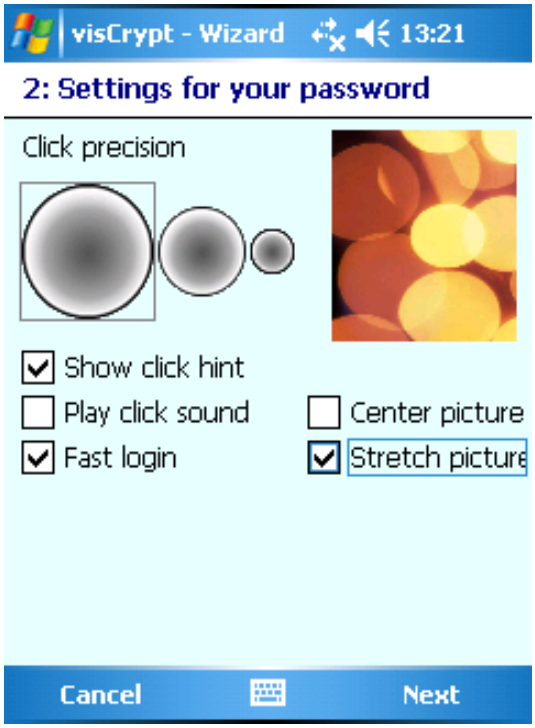
If you are using visCrypt the first time or you want to change your master password, visCrypt will guide you through the process of password definition step by step.

First you must select the password type (login type).

If you chose the picture password, you have to select a picture you want to use for your password.

visCrypt offers some pictures for different screen resolutions. Of course you can use your own pictures, too.

visCrypt accepts pictures in JPG format.



In the second step for your picture password you can change additional settings now.

In "click precision" you can set, how precise you must hit the selected spots in the picture. The size of the circle illustrates the spot area. Smaller click precision provides a more secure password.

"Show click hint" shows a small symbol at the clicked position in your picture for control.

"Play click sound" activates playing a sound on every click in the picture.

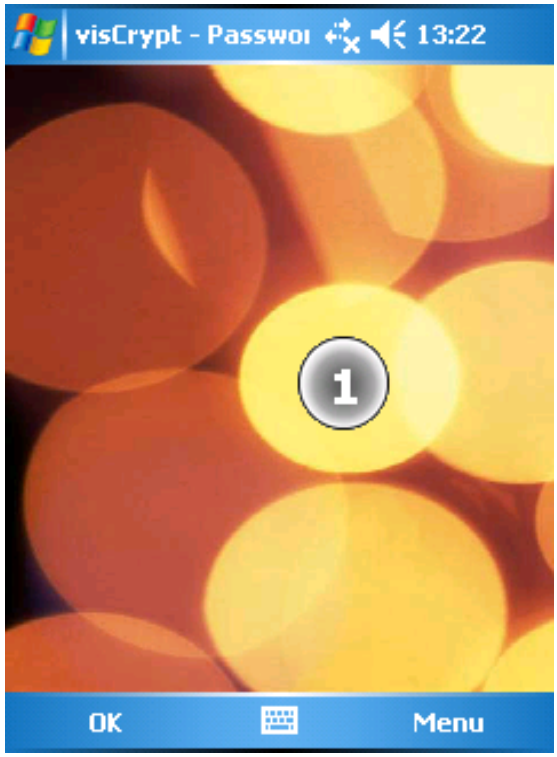
If you activate "Fast login", then a password will be regarded as correct after entering the last correct spot without confirmation.

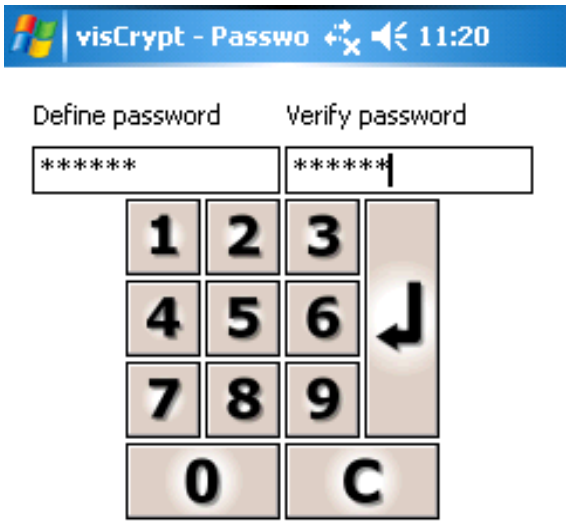
"Center picture" and "Stretch picture" changes the drawing behavior of your picture, if it does not fit into the screen optimally. The preview picture illustrates the effect.

At last you must define your new password.

For a picture password just click several spots in the picture in a defined order and confirm with “OK”.

You must reenter the password to let visCrypt accept and the save the new password.

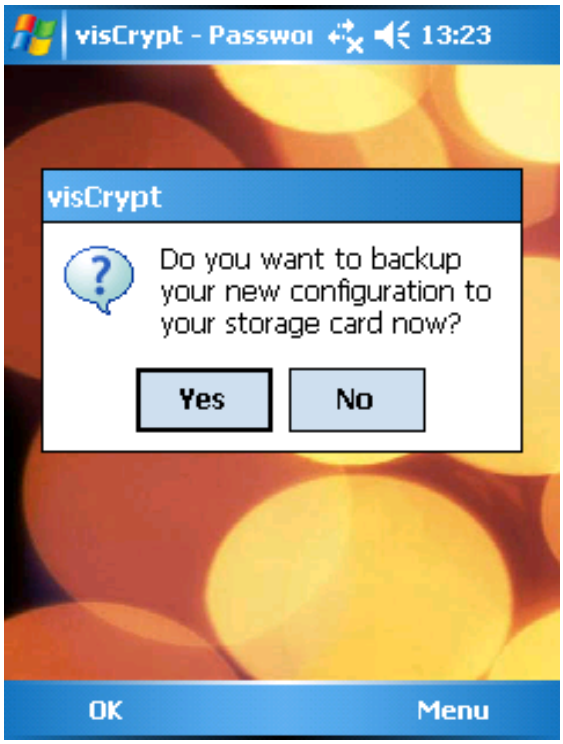




For a PIN password visCrypt offers a number pad for entering the password quickly.

If you use a text password you can use the virtual keyboard of your Windows Mobile Device.

The configuration file of visCrypt



After defining your first or a new master password, visCrypt refreshes the configuration file. Your master password and this configuration file is necessary for visCrypt to decrypt your files and documents.

The password file is named "**visCrypt.conf**" and is laying hidden in the folder "My Documents" on your Windows Mobile Device. You can see this file over a connection on your PC and take a copy there.

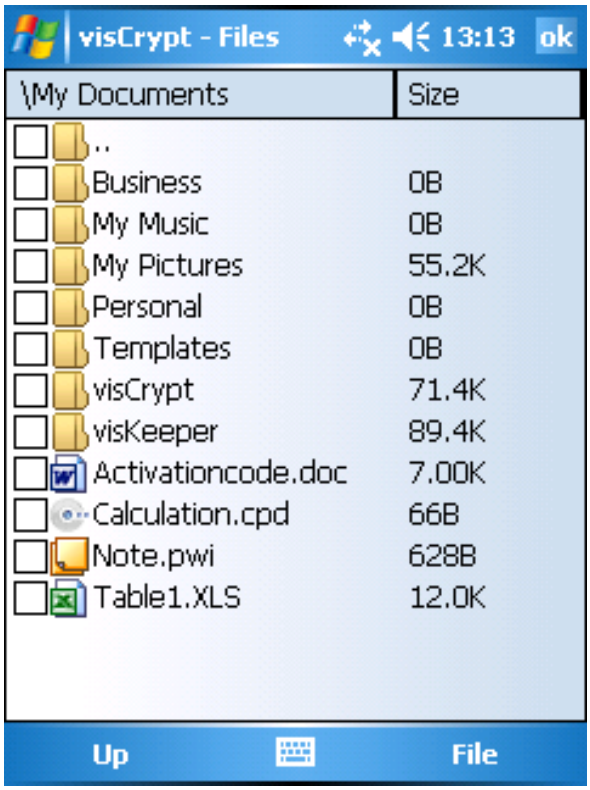
Please store an actual copy of this file **outside of your Windows Mobile Device**, to be able to decrypt your files (maybe on a storage card) even after a hard reset of your Windows Mobile Device.

You should always backup the configuration file after changing your password.

If your devices has a storage card, visCrypt asks to backup your configuration file automatically after successful password definition. The backup is located in the folder "visCrypt_Backup" on your storage card afterwards.

The main screen

The list view



The main screen contains a table (list view), that shows the contents of the currently selected folder. There are up to three columns. The first column shows the filename or the folder name. The second possible column shows the file date, if this column is activated in the settings. The third possible column shows the file and folder size, if this column is activated in the settings.

When clicking the column header you can change the sorting of the list entries, while the folders remain on top.

Navigation is quite easy:

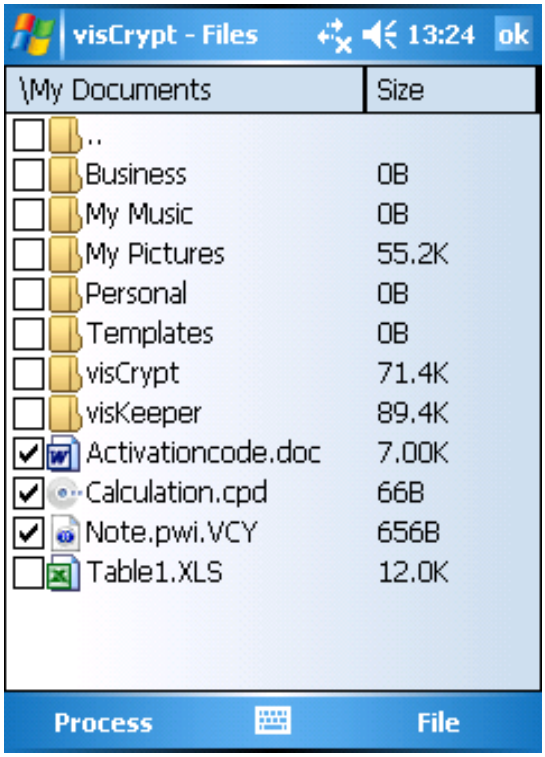
- Click on a folder to show its contents
- Click on the top folder (“..”) to change to the parent folder

The table header shows the name of the current directory

To encrypt a file just mark the check box beside and click on "Encrypt" in the menu bar.

Decryption is done similar.

If you have marked both, encrypted and decrypted files, click on "Process" in the menu bar. The files then are being processed according to their state.

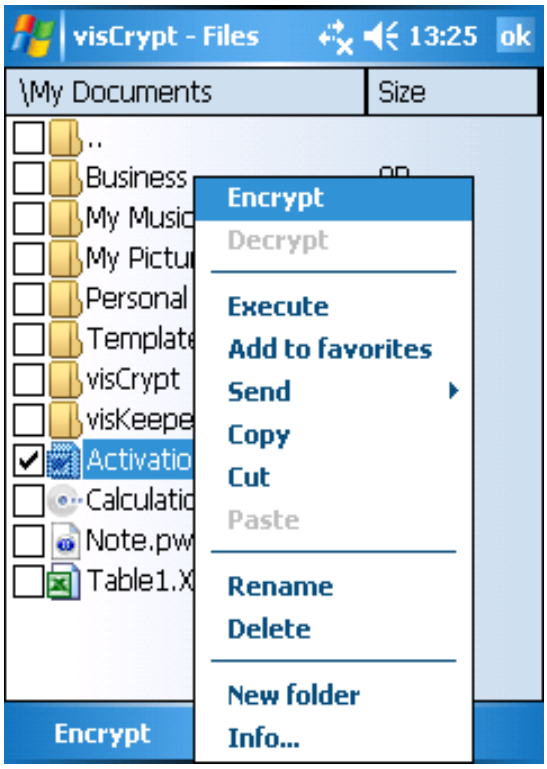


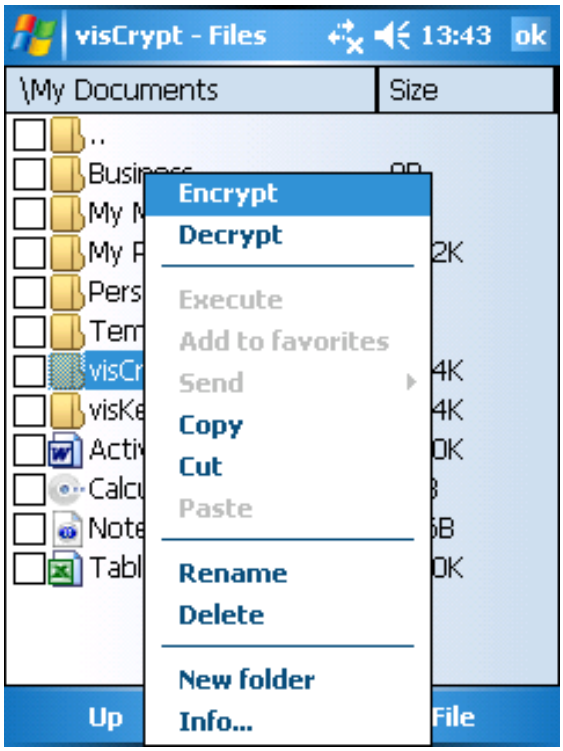
The context menu of the list view

Many features of visCrypt are available using the context menu of the list view.

If you open the context menu for a file, visCrypt offers the following functions:

- Encrypt or decrypt the selected file (according to its state)
- Execute the file
- Add the file to your Favorites
- Send the file
- Copy, Cut and paste the file
- Delete and rename the file
- Create a new folder
- Show file information (see below)





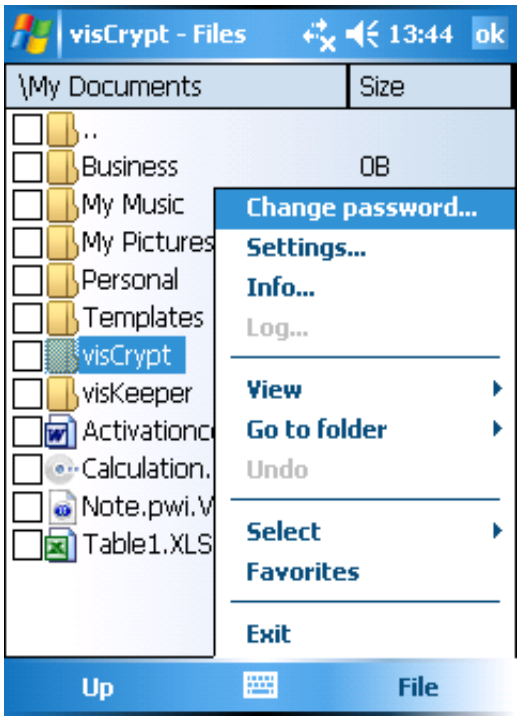
If you selected a folder and open the context menu, you can:

- Encrypt the folder (this means encryption of all files in this folder and all sub folders)
- Decrypt the folder (this means decryption of all files in this folder and all sub folders)
- Copy, Cut and paste a folder
- Rename and delete a folder
- Create a new folder
- Show folder information (see below)

The context menu can be opened by clicking and holding on a file or folder.

The file menu

General

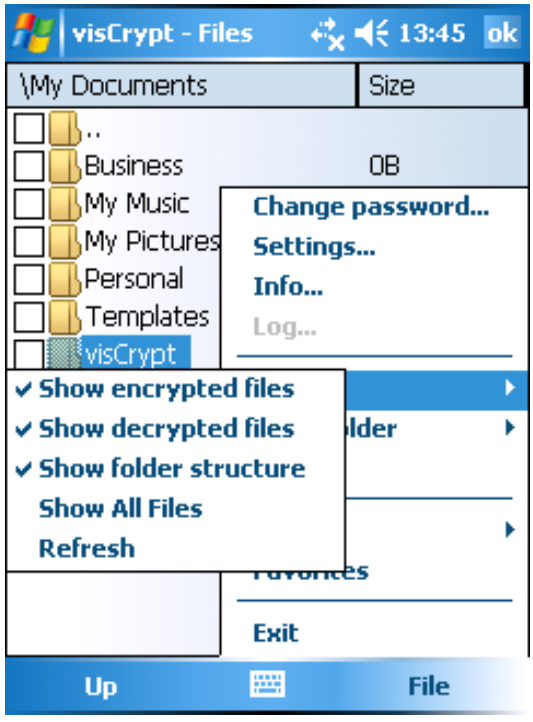


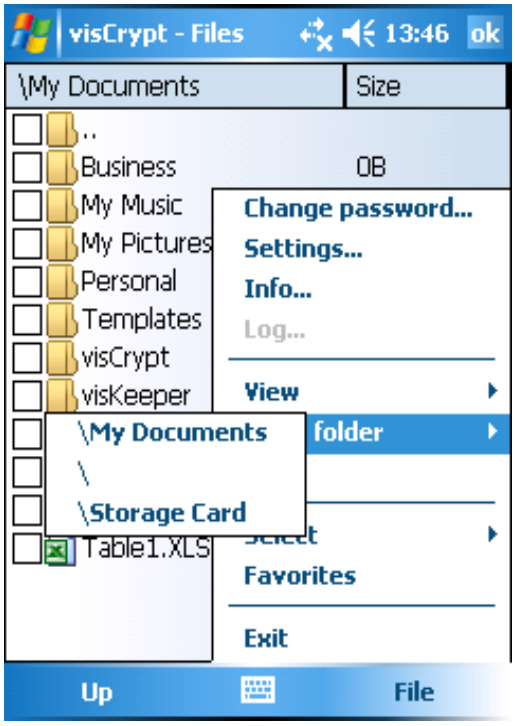
In the file menu you can find additional functions for the list view of visCrypt and more:

- With “Change password” you can enter the password wizard screen to define a new master password.
- In the submenu Selection you can “Select all files” or “Clear selection”.
- With “Exit” you can leave visCrypt.

In the “View” menu you can change the shown content of the list view:

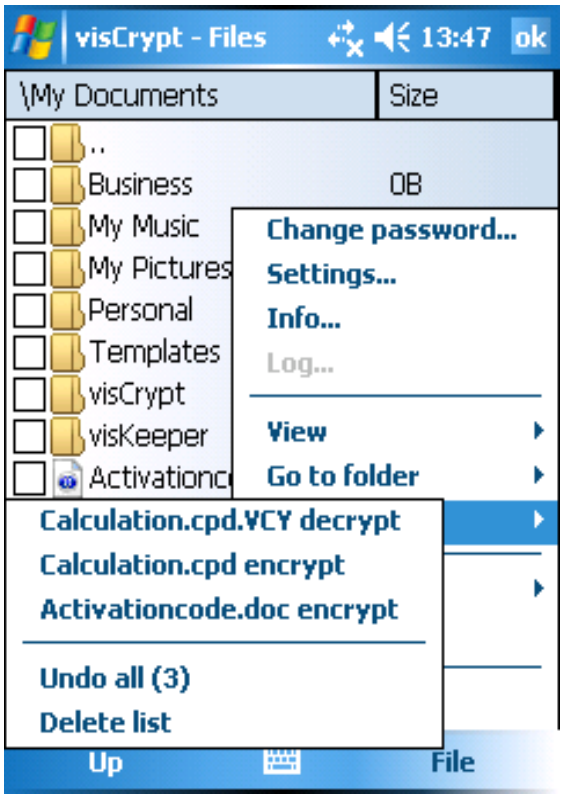
- With “Show en-/decrypted files” you can filter the list view contents for files with the selected state.
- If you deactivate “Show folder structure”, all files of all folders are being displayed in the list view. So you don't need to navigate through subfolders.
- “Show all files” shows hidden files, too.
- “Refresh” reads the current folder's contents again.

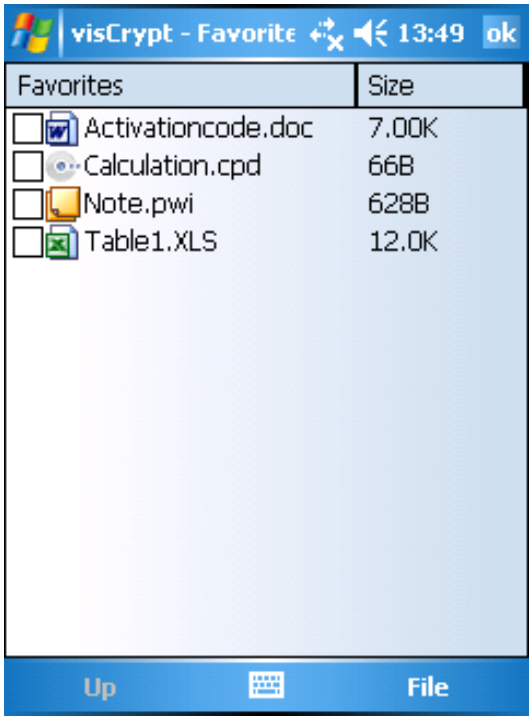




In the "Go to folder" menu you can see the last shown folders and open them simply clicking a folder name there.

In the "Undo" menu you can see the last encryption actions and undo them step by step or all together.





With the menu item "Favorites" you can change to Favorites view.

In this view only special selected files are shown. You can add any files to Favorites view from the normal list view.

So you can manage all your important files in one single view without navigating through the folders.

If you do not already have a Favorites list, visCrypt asks you to search for favorite (encrypted) files, which then are added to your Favorites automatically

The size of the Favorites list is limited.

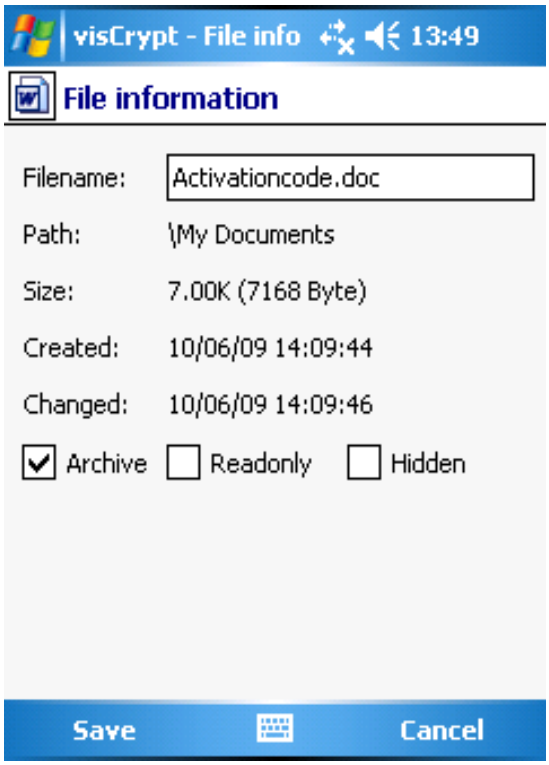
Information for files and folders

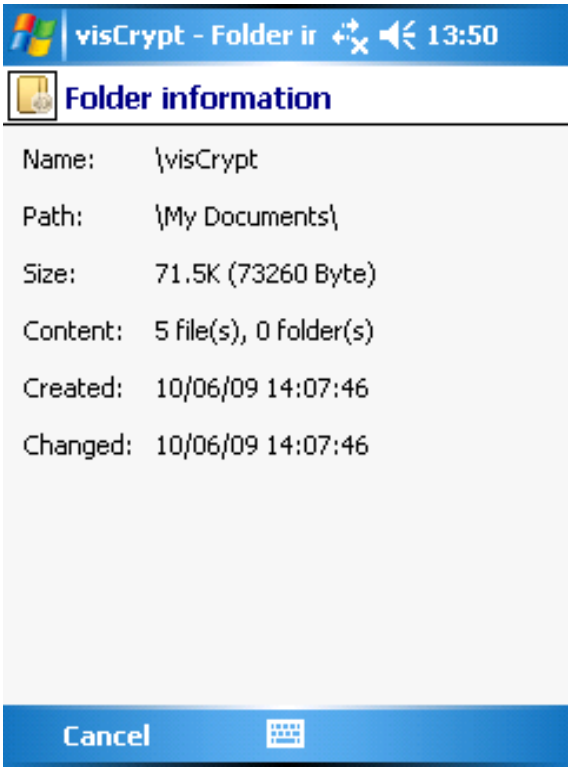
In the context menu of a files you will find the item "Info".

Selecting this item will open a new screen showing information about this file.

Some of this information can be changed and saved, like filename and file attributes.

This screen can also be reached via the file explorer's context menu and without entering the master password.





In the context menu of a folder you will also find the item “Info”.

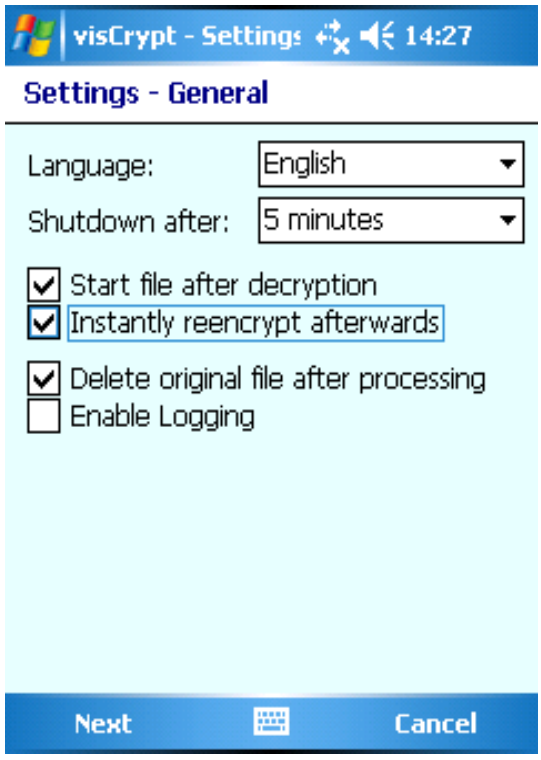
Selecting this item will open a new screen showing information about this folder.

This screen can also be reached via the file explorer's context menu and without entering the master password.

Settings

In the settings screen you can set your preferred options for visCrypt.

The “general” page contains:

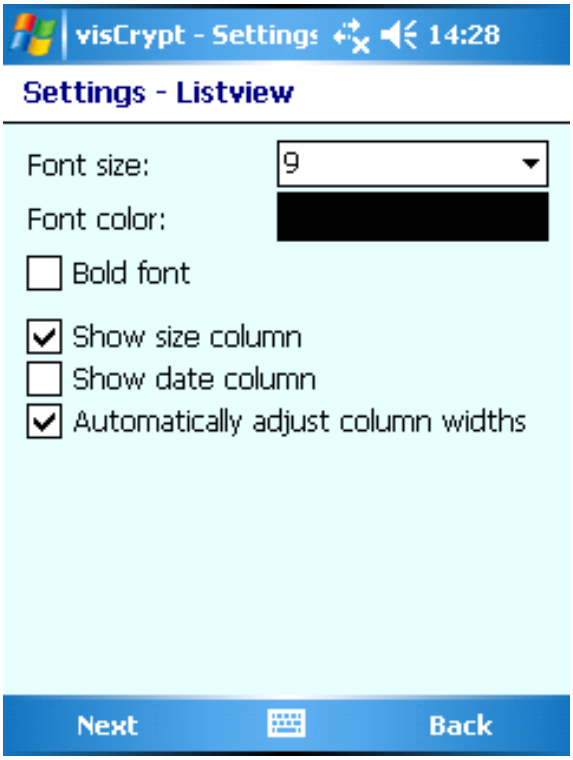


- Language: Select the language for the user interface.
- Shutdown after: Select, how long visCrypt will stay opened without activity.
- Start file after decryption: If activated, a decrypted file (in windows file explorer) will automatically be started with the linked application.
- Instantly reencrypt afterwards: If activated, a decrypted and opened file will be reencrypted after closing the file automatically
- Delete original file after

processing: If a file gets en-/decrypted, the "original file" will be deleted on success.

- Enabled Logging: If activated, all important actions in visCrypt will be documented in a log file.

With „Next" you can proceed to the next settings page.



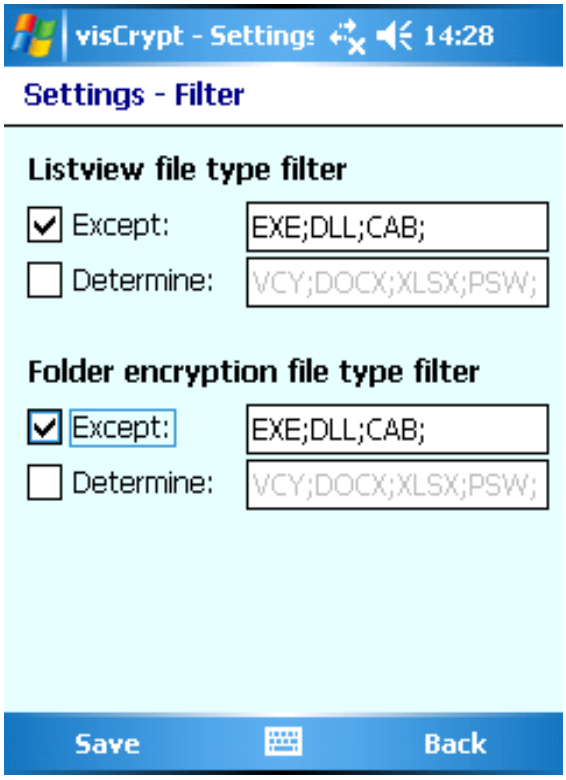
The "listview" page contains:

- Font size: Set the font size of the list view in the main screen of visCrypt.
- Font color: Click the color bar to open a color screen to select the listview font color
- Bold font: Will activate bold font for the listview
- Show date column: Will activate the date column in the listview
- Show size column: Will activate the size column
- Automatically adjust column widths: Will fit the column widths into the screen width automatically

With „Next" you can proceed to the next settings page.

The "filter" page contains:

- Listview file type filter: With this filter you can make visCrypt show only specific file types ("Determine") in the listview or not show specific file types ("Except")
- Folder encryption file type filter: With this filter you can make visCrypt encrypt/decrypt only specific file types ("Determine") or not encrypt/decrypt specific file types ("Except")



With "Save" all changes will be saved to disk. visCrypt needs to restart to get all new settings up and working.

Information and activation

visCrypt - Info 14:29
visCrypt Version 3.0.0
© 2009 SFR GmbH
Protect your files easy and effective with visCrypt.
First select a login type and define a new password.
Now you can select files from the list and encrypt these files with a single click.
Decryption of a file can be done within visCrypt or even in the file explorer of your Windows Mobile device.
OK
Activation ...

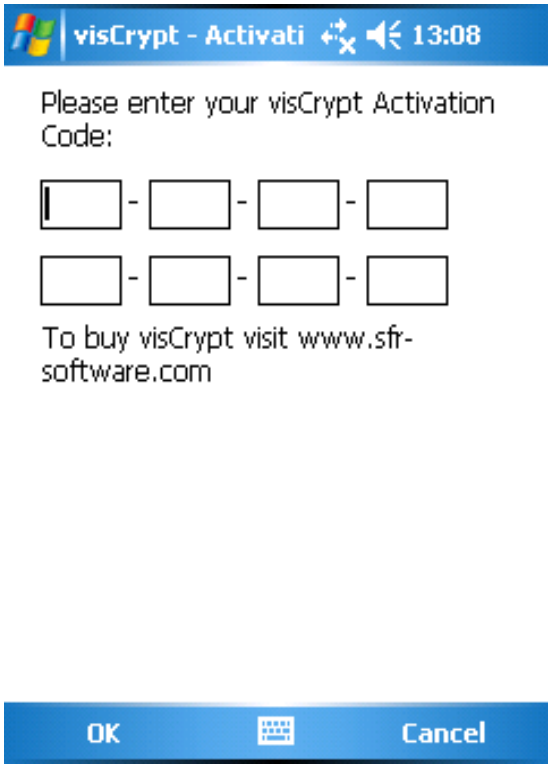
The menu item "Info" in the file menu of visCrypt opens an information screen. You can find version information of visCrypt and a short description and manual of the program here.

The second menu item of this screen opens the activation code screen.

Enter your purchased license key in this screen to register visCrypt.

You can use the virtual keyboard or another input method. Confirm your input with "OK" afterwards.

If you mistyped the code, please correct your input and confirm again.



Log

visCrypt - Log 1:42
Log
6/20/2007 2:41:29 PM Successful login
6/20/2007 2:41:56 PM Encrypted \My D
6/20/2007 2:41:59 PM Decrypted \My D
6/20/2007 2:42:08 PM Decrypted \My D
6/20/2007 2:42:09 PM Encrypted \My D
6/20/2007 2:42:26 PM Changed passwo
6/20/2007 2:42:35 PM Decrypted \My D
6/20/2007 2:42:39 PM Encrypted \My D
Cancel

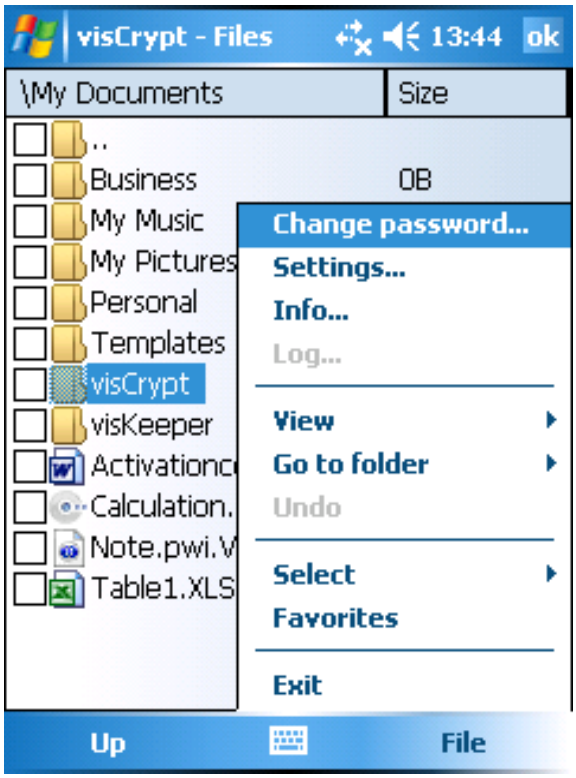
visCrypt can log all important actions into a log file to control usage later on.

The log function needs to be activated in the settings screen of visCrypt.

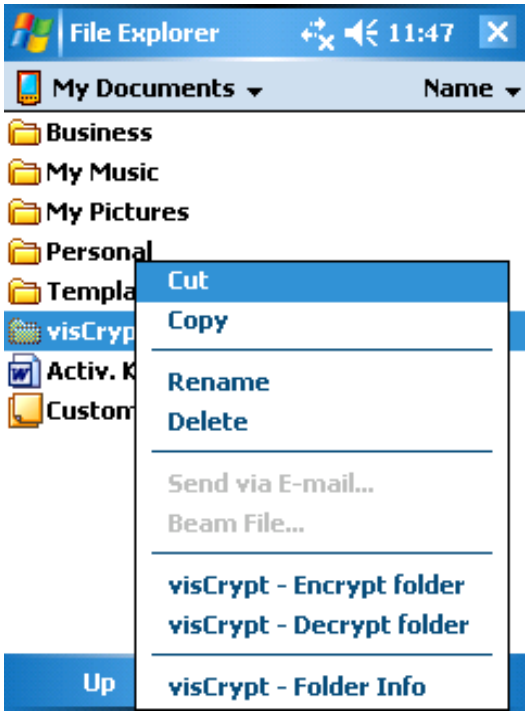
Close visCrypt

visCrypt can be closed in different ways.

You can click on "OK" in the top right corner of the main screen or select "Exit" in the file menu of visCrypt.



Integration into Windows Mobile's file explorer



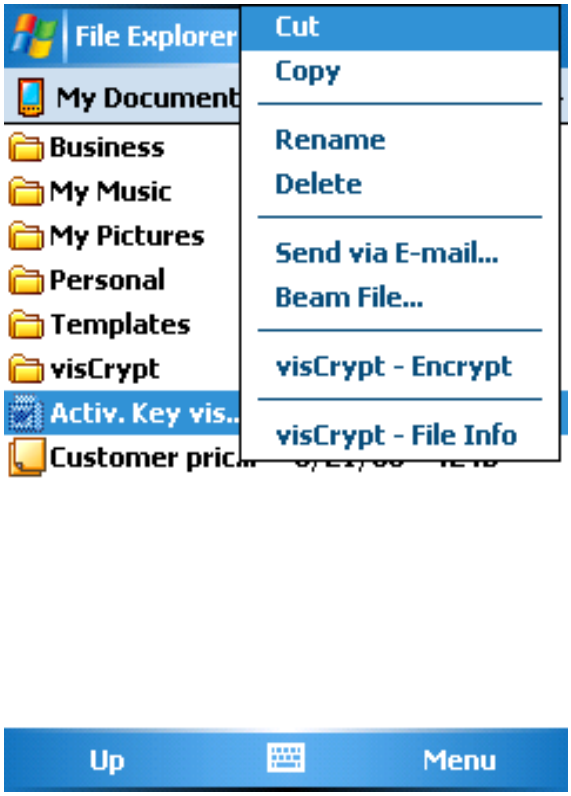
visCrypt integrates into the context menu of the file explorer of Windows Mobile to give you even more flexibility in using the encryption functions of visCrypt.

According to the type of selected object (file or folder) you can see the adequate functions of visCrypt when you open the context menu.

Of course you need to enter your master password to run the selected function.

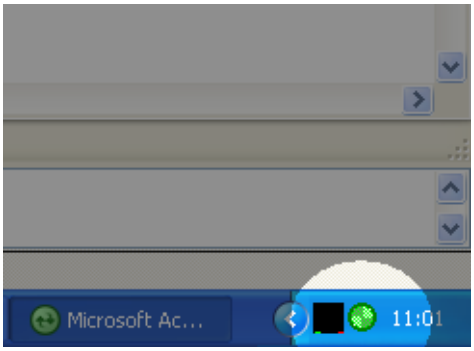
The info function works without password entry.

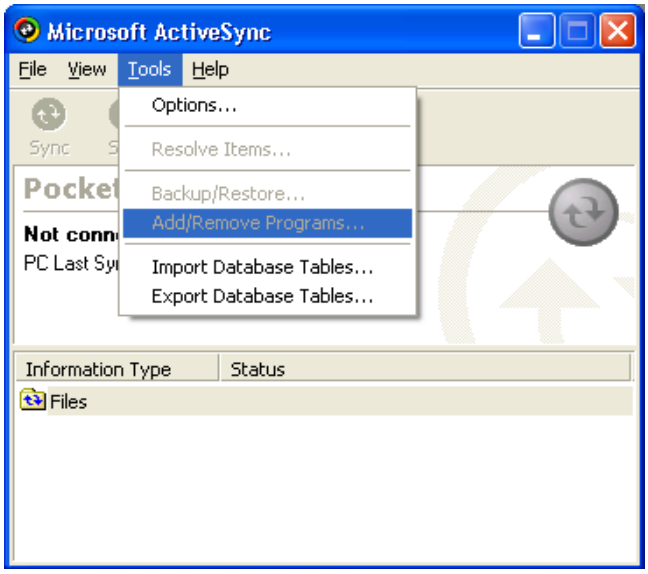
If you have activated the setting “Start file after decryption”, the decrypted files will be opened automatically in the linked software application.



Uninstall visCrypt

If you want to uninstall visCrypt, you should do this just like in the installation process using an ActiveSync® interface.





In Windows XP:

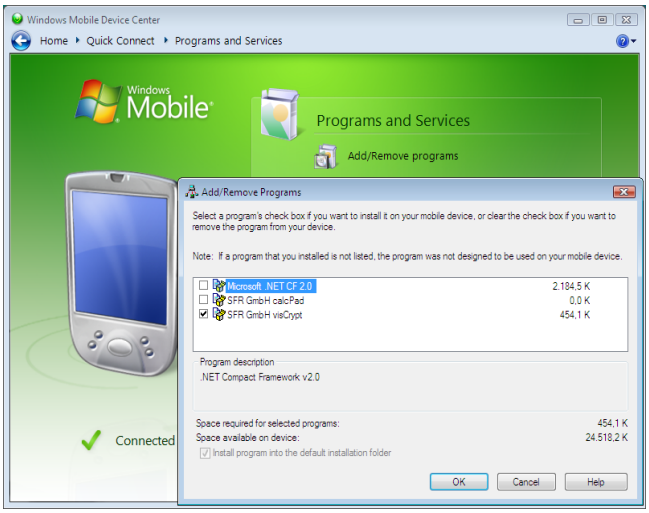
Start the ActiveSync-software with a double click on the symbol in the task bar.

Call up the option "**Add/Remove Programs...**" in the menu "**Tools**".

In Windows Vista:

Start the Windows Mobile Devicecenter.

Go to the menu “Programs and services” and then open the menu “software”.



Deactivate the control box beside the entry "**SFR GmbH visCrypt**" in the following dialog box by clicking on the checkbox to delete it.

Click on "**Remove" or "OK"** to start the uninstall process.

If you are sure you want to remove visCrypt confirm the following message with **"OK"**.

visCrypt will now be deleted completely from your Windows Mobile Device. If you want to use visCrypt later on to protect your data, you will have to reinstall the software as described in the chapter "**Installation"**.

The patented visual Key technology

Most operating systems and many programs require that the user identifies himself. Usually this is effected by typing in a text password. For security reasons these passwords should not be created associatively (NOT the children's first names, NOT the wedding day, etc.). Furthermore, the passwords should be changed regularly.

Thus most computer users have to memorize several difficult and ever changing passwords. This results in severe safety gaps, as many users either ignore these rules or note their passwords down.

visual Key: An alternative to text passwords

The disadvantages sketched above may be eliminated in an economical and uncomplicated way by the use of passwords based on images. It is much easier for humans to remember pictures (or parts of pictures) than text. Furthermore, associations with pictures are more variegated and individual.

The input of a visual password is effected by selecting several spots in an image (e.g. by tapping with the stylus). There are more advantages to this method:

- This procedure is not limited to systems equipped with keyboards but may also be employed on touch screens or kiosk systems.
- In comparison to other methods, such as biometric identification technologies, generally no additional hardware is required to employ it, since virtually all today's computer systems are equipped with a mouse or other input device.
- Contrary to biometric identification technologies, there is no direct correlation between the identification and the person identifying. Several persons may even use the same password.

The process

As a first step to define a password the user chooses an image. This may be any picture, but ideally it should have a multitude of distinguishable details. Then the user selects one or more spots in the picture by stylus tap or using another input device. The password (the visual key) will be created from the selected points and their order.

© 2009 SFR GmbH, Cologne, Germany

The chosen details and their sequence are easy to remember. Additionally, the picture itself helps the user to form individual associations ("there is a BOAT on the RIVER, passing a MAN wearing a HAT").

In order to identify himself to the system later on, the user just has to pick the selected spots in their original order in the given picture.

Technical implementation

Before generating the password the program divides the selected picture (not necessarily visible to the user) into cells. The number of created cells forms the maximum character set (the "alphabet") for the password, each cell representing a single character.

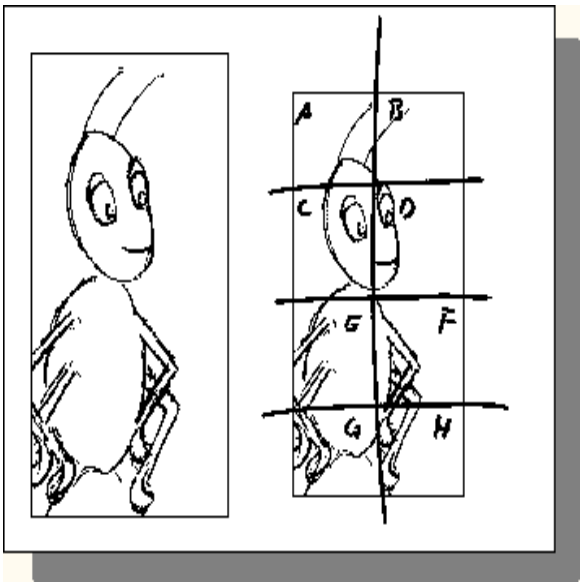
In order to define a password, the user may select any desired spots in the picture: The character of the cell belonging to the spot will be transferred to the password.

Later on, the user identifies himself by choosing the same order of points, thus composing the same password again.

There are two different procedures to divide the image into cells:

1. Regular allocation

The image is divided into regularly sized cells (e.g. rectangles or hexagons). When defining a password this grid is shifted with each input so that any selected spot is situated exactly in the center of a cell. This serves to compensate the inevitable "fuzziness" of later input.



Since it is as good as impossible to hit exactly the same spots (pixels) again when entering the password, this shifting of the entire grid defines the whole cell as valid input area, thus permitting small deviations in any direction.

Apart from the graphic, the cell size and the offsets of all grid shifts must be

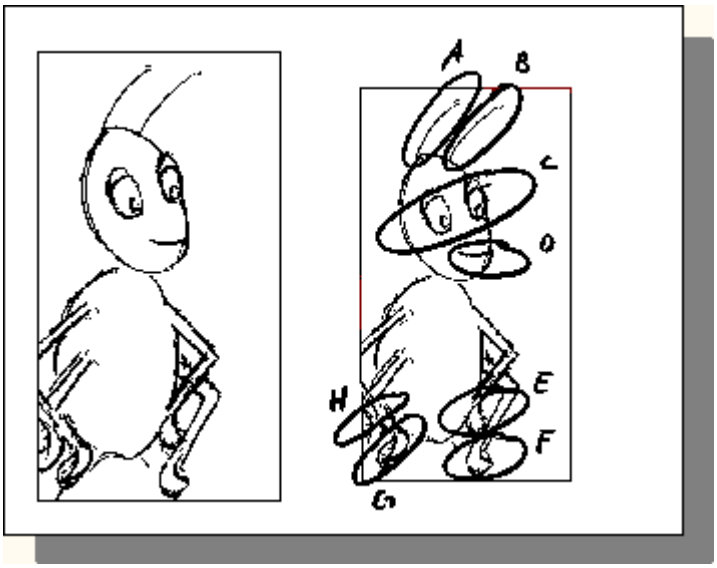
stored. All this information will be needed to generate the correct password from the user's input. However, it is neither necessary nor wanted to store the password itself.

The security of the password depends on the cell size as well as on the width and height of the underlying graphic, since these data determine the total number of cells and thus the range of the alphabet.

The regular allocation procedure is used by visual Key PPC. Additionally, for each touch the first cell's value is randomized and stored. Thus the first cell does not always represent the character "A" but may contain any character.

2. Irregular allocation

With the irregular allocation of a graphic its particularities can be taken into account (distinct points, individual symbols, remarkable areas). In this case the allocation is done either manually or with appropriately "intelligent" programs. In contrast to the first procedure there is no unspecific fault tolerance. Therefore the user and the creator of the mask have to agree upon how certain symbols shall be analyzed (e.g. "edge or surface").



In addition to the graphic the complete mask (the alphabet) must be stored. Again the security level of the password is dependent on the range of the alphabet (total number of defined areas).

This procedure is currently not supported by our visual Key products but may be subject to future enhancements.

License Agreement

visCrypt

Version 3.0.0

Copyright © 2009 SFR Gesellschaft für Datenverarbeitung mbH, Cologne, Germany, All Rights Reserved

Please read the following terms and conditions before using visCrypt. In the event that you use this software, you are agreeing to be bound by the terms and conditions of this agreement. Should you not agree with these terms, do not use visCrypt.

A single user license permits the use of visCrypt on a single computer. Multiple user licenses will be subject to the terms and conditions granted in such license.

COPYRIGHT

The software visCrypt and the documentation are owned by SFR and are protected by copyright laws and international treaty provisions. No title to intellectual property is being transferred. You may not modify, reverse engineer, decompile or disassemble the software. You may not translate, reverse engineer, decompile, disassemble, modify or patch the visCrypt executable files or documentation in any way.

LIMITED WARRANTY

SFR warrants that the program will perform in substantial compliance with the documentation supplied with the software product. If a significant defect in the product is found, the Purchaser may return the product for a refund. In no event will such a refund exceed the purchase price of the product.

Limitation of Liability: EXCEPT AS PROVIDED ABOVE, YOU AGREE THAT SFR SHALL NOT BE LIABLE, UNDER ANY LEGAL THEORY, INCLUDING TORT, CONTRACT OR OTHERWISE, FOR ANY DAMAGES INCURRED BY YOU INCLUDING BUT NOT LIMITED TO DIRECT OR INDIRECT DAMAGES FOR LOSS OF GOODWILL, LOSS OF DATA, BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR OTHER COMMERCIAL OR PECUNIARY LOSS, ANY CONSEQUENTIAL, SPECIAL OR INCIDENTAL DAMAGE) OR ANY OTHER PERSON OR ENTITY AS A RESULT OF YOUR USE OR INABILITY TO USE THE SOFTWARE OR DOCUMENTATION EVEN IF SFR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME

JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU.

GENERAL

This Agreement is the entire agreement between SFR and you, supersedes any other agreements or discussions, oral or written, and may not be changed except by written amendment signed by the author of this product. This Agreement shall be governed by and construed in accordance with the laws of Federal Republic of Germany, excluding its conflict of laws, rules and the United Nations Convention on Contracts for the International Sale of Goods. If any provision of this Agreement is declared by a court of competent jurisdiction to be invalid, illegal or unenforceable, such provision shall be severed from this Agreement and the other provisions shall remain in full force and effect.

Should you have any questions concerning this license agreement, or if you desire to contact the author of this product for any reason please e-mail SFR at support@sfr-software.com.

Windows®, ActiveSync®, Windows Mobile® are registered trade marks of the Microsoft Corporation.